2018

SHOOT IT.SOLUTIONS

Switching papers

Written by:
Eng.
Amgad M. Mesallam
Edited by:
Eng. Abeer Hosni

"Switching"

Chapter 1:-

"Layer 2 devices"

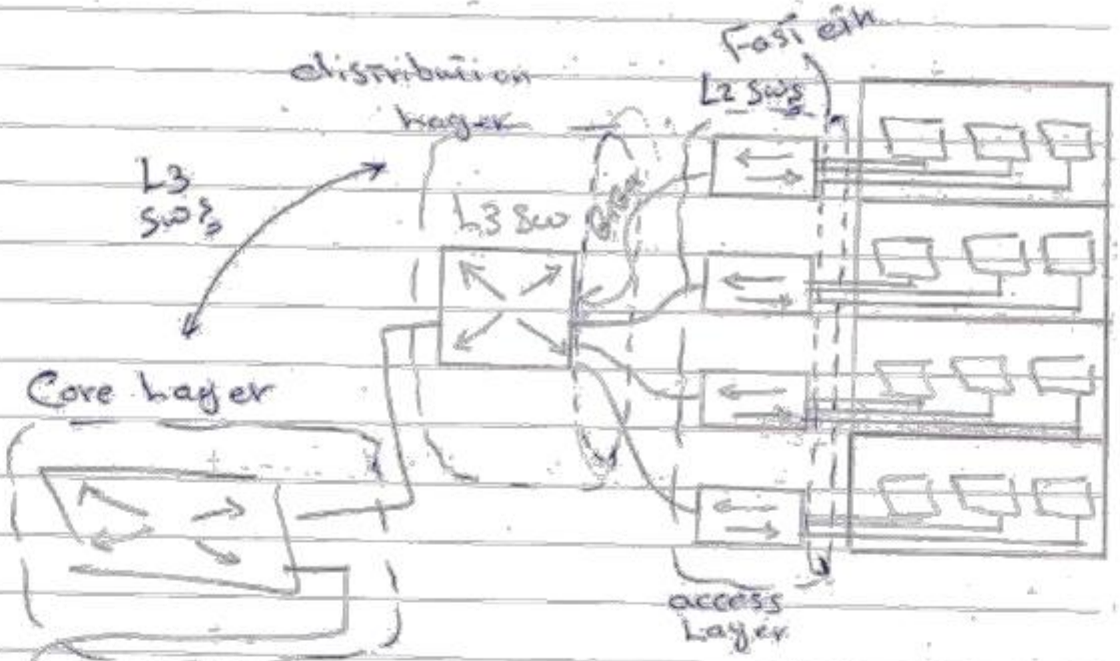
A layer 2 device is a device that understand MAC, for ex:-

* NIC (Network Int. Card)
* Bridge
* switch: Multi-port ~~s~~ bridge
  up to 256 port

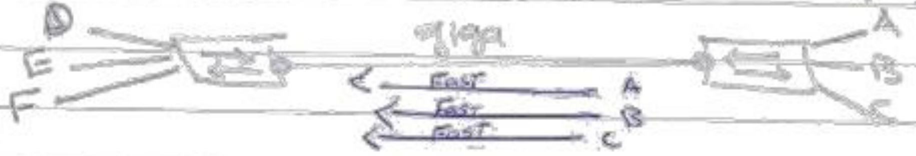
علشان اربط شبكة في نفس الـ network ID => switch
باستخدم الـ switch
لو الـ network ID مختلف باستخدم الـ Router

- الفرق بين الـ bridge والسويتش أن الـ bridge يتعامل
مع الداتا كـ software وبالتالي هو جهاز بطيء ولكنه يقسم الشبكة
لـ broadcast domains ، بينما السويتش يستخدم الـ ASIC لنقل
الداتا وبالتالي يتعامل معها كـ hardware وبالتالي يرسل الداتا بسرعة
الـ int (أي جهاز سريع) وهو كذلك يقسم الشبكة لـ broadcast
domains.

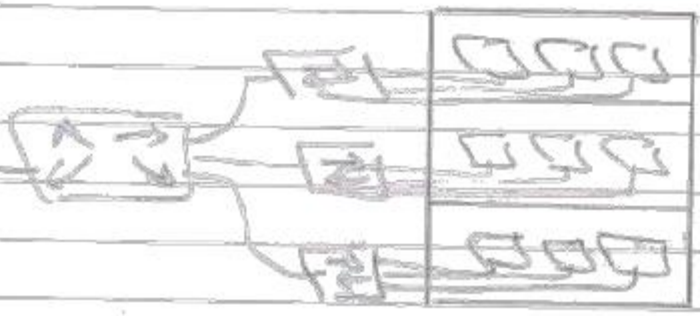
I Hierarchical Network Design



Recommended ⇒ Connect 2 switches by giga eth.
or 10 giga eth



⇒ 24 Port Fast eth
2 Port GiGa eth



وكان الـ Hierarchical Network design لم يشرح كيفية ربط
الشبكة بالإنترنت. لذلك قاموا بعمل model آخر
هو Cisco enterprise architecture، وهو يتكون من :-

Cisco enterprise architecture :-

1. enterprise Campus (access + distribution + Core + server farm)
2. enterprise edge (the internet Connectivity)
3. service provider edge (ISP)
4. Remote (like VPN users).

---

* In-Band (IB)

معناها عمل Connect على الراوتر باستخدام tool مثل الـ telnet
أو الـ SSH أو الـ HTTP.

* out-of-Band (OOB)

معناها عمل Connect على الراوتر باستخدام الـ Console أو الـ AUX
واستخدام terminal emulator لعمل الـ Connect عليه.

---

* link aggregation :-

تجميع العديد من الـ links في bundle واحدة لزيادة الـ BW.

Cisco ⇐ Recommend ⇐ لو هعمل Configuration لقدر
بالإمكان اكون في الـ Access layer لو لدينا نقص تحكم
في الـ Distribution أكثر من البعض في الـ Core

* Scalability :- Hierarchical Network
Can be expanded easily

* Redundancy :- at the Core and distribution level ensure path availability.

أكثر من طريق علشان اوصل من الـ Source للـ destination

* Network Diameter :-

عدد الأجهزة اللي بتعدي عليها الـ Data علشان توصل من الـ Source للـ destination.

* What is the Converged network

شبكة تحتوي على كل أنواع الـ traffic مثل الداتا والـ VoIP والـ video وغيرها.

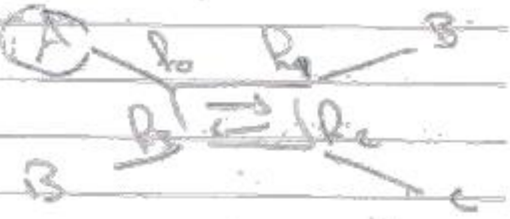
Chapter 2:- (Switching)

الفرق بين الـ hub والـ Switch

CSMA/CD

بيعمل Flood يرسل الى كل الشبكة ما عدا الجهاز منه
لـ Data (يقوم بعمل flood على كل الـ ints ماعدا الـ int اللي استلم منه الداتا)

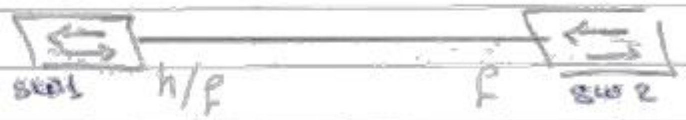
أول frame بيعمله flood فقط ويعرف بيني الـ
Mac-address-Table
موجود بـ RAM



Mac-add-table

	int	MAC	
أول Source	Fa0	A	← aging-time
ثاني Source الموجود	Fa2	C	

اي عنصر جوه الـ Table بيفضل لفترة اسمها aging-time
لفترة By default ← 300 sec



Communication modes-

- single ⇒ (Radio)
- half duplex ← ☁ ← بيعتمد شغل على نفس

السلك ومعرض لل Collision بيستخدم الـ CSMA/CD

- full duplex ⇄

بيبعت على سلكة واستقبل على سلكة

وبالتالى لا يحتاج الـ CSMA/CD.

by default auto nogotiation ⇐ Switch ال

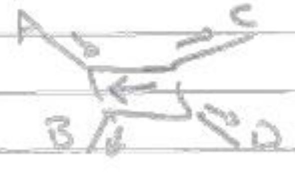
* لو جالي sw1 auto و sw2 full هيشغل CSMA/CD على sw1 half

* Broad Cast domain

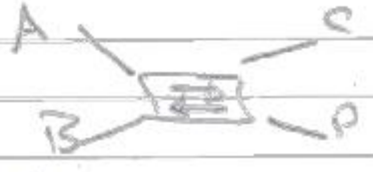
النطاق اللى هيسمع منه الـ Broadcast

for hub ⇒ 1

for sw ⇒ 1

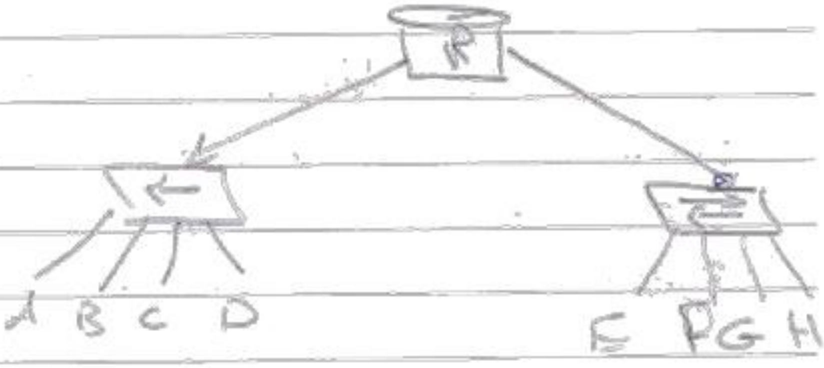


* Collision domain



for hub ⇒ (1)

for sw ⇒ No of ints

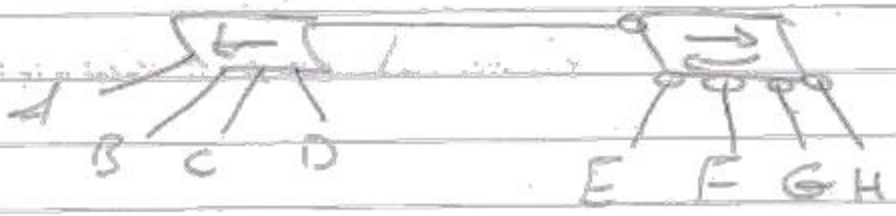


Broad Cast domain (2)

Collision domain

for hub => 1

for sw => 5 ==> (6)



Broad Cast domain = (1)

Collission domain = (5)

* Switching Modes:

* Store and forward

معناه ان ال Data اول ال frame هيجي لل Switch

وبعده هيجمعها كلها مايبعت هي ال frame كاملة

وهي 1500byte وبعدها هيبعتها لل Destination

* مشاكلها انه بطيء

* Cut-Through

ال frame الي بتوصل بيبعتها لل Destination (bit)

على طول

مشاكلها ان ال FCS = check sequence frame

موجودة في اخر 64byte من ال frame.

علشان كده مش بتعرف انه يعمل check sequence.

- Fragment offset

ال Switch هيجمع اول 64b وبعدها يبعتها

علشان يكون عنده إمكانية لـ FCS ويعمل عن طريقها

Error Detect

* في ال fragment offset بما إن السويتش هيجمع أول 64byte

طريقة ال store and forward وده حتى يكون عنده القدرة على عمل

detect لل error بطريقة ال FCS ، وبعد ذلك باقي ال frame

هيتعامل معاه بطريقة ال cut-through .

Switch boot sequance:-

* The boot sequance of Cisco switch:-

- the switch loads the boot loader software from NVRAM
- the boot loader:-
  - Performs Low-level CPU initialization
  - Performs POST
  - intialize the flash file system
  - loads the o.s image into the RAM

* ال flash بتاع ال Switch جواه

① The ios of the switch

② the VLAN data base

③ the Configuration file.

* The Switch uses the NVRAM to store two types of file

① Start-up Config
② The boot Loader.

Labs. Password recovery

"Switch"

مش بيشتغل على GNS وال Packet Tracer

الخطوات: ① باعمل "Reset" هاشيل كابل Power

دا البوتاني وضغط 15sec هاضغط على زرار Mode

وهلاقي ⟸

switch: Flash_init ↵

switch: Load_helper ↵ ⟸ يعمل [illegible]

initialization لل flash

وال password بيبقى موجود جوا ال flash في ملف اسمه

Config.TEXT

ال switch أول ما بيقوم لازم يلاقي ال Config.TEXT

switch: Rename Flash:Config.TEXT Flash:

Config.old ↵ أمر ٢

: boot

هيعمل boot مش هيلاقي ال Config.TEXT

وبالتالي هاعتبر أول مرة اشغل ال switch وبعدين هرجع اسم

ال Config.old ⟸ لاسمه الأصلي ⟸ Config.TEXT مرة تانية

اقدر اغير ال Password

sw# rename flash: Config.old flash: Config.text

sw# dir flash:

sw# Copy flash: Config.text system: running_Config

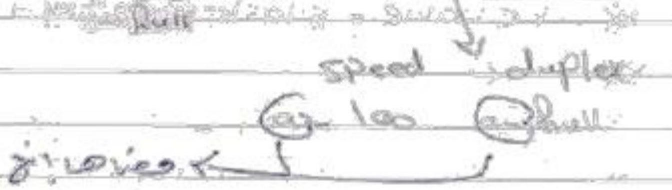
```
Switch> ena ↵
Switch# Configer T ↵
sw(Config)# hostname sw
sw(Config)# line ConsoLO ↵
(Config-line)# Password ____
(Config-line)# Login
(Config-line)# do wr
(Config-line)# Exit ↵
```

SW #show interface status ↵ بيظهرلي حالة الـ Int
كلها

متعلق بـ Duplex والـ speed ⇐ متسوية auto
خاصة بـ Type ⇐ 10/100 يعني يعمل السرعتين
ولو اتنين لو كان Giga هتلاقيه 10/100/1000 يعني
هيعمل بـ ٣ سرعات وبعضهم عن طريق الـ speed ...

```
Cisco (config-if)#speed 100↵
Cisco (config-if)# duplex full↵
```

غيرت السرعة بتاعة الـ Int من Auto لـ 100 وبدل duplex من Auto لـ full



← هيعمل ... عن طريق auto-negotiation.

(Note لما تشغل على hard code الـ duplex على واحد الـ سويتش وتركه على auto negotiation على السويتش الآخر.

* ليه عشان احط IP على ال Switch ؟

- علشان ان لو حبيت اعمل Connect Remotly عليه عن طريق ال Telnet أو ال SSH .

Switch(Config)# interface Vlan 1 ↵

sw (Config-if)# IP add 10.10.10.10 255.255.255.0↵

sw(Config-if)# No shutdown↵

sw (Config-if)# exit

sw (Config)# IP default-gatway 10.10.10.1

* ليه باحط Gatway على ال Switch ؟؟

- علشان انا لو بعيد اعمل Connect عليه عن طريق ال Telnet من بره الشبكة بتاعتي

Switch# Config t

(Config)# line Vty 0 4

(Config-line)# Password Cisco

(Config-line)# Login

(Config-line)# end

SSH

Secure Shell (22) Port

Telnet ⇒ Clear text
SSH ⇒ encrypted data
VPN ⇒ Tunneled data

R1
(Config) # Int Fa0/0
R1(Config-if)# IP add 10.0.0.1 255.255.255.0 ↵
R1(Config-if)# No shutdown

R2
R2(Config) # Int Fa0/0
R2(Config-if)# IP add 10.0.0.2 255.255.255.0 ↵
R2(Config-if)# No shutdown
R2(Config) # line Vty 0 4
R2(Config-line)# Login Local
exit
R2(Config)# username abeer privilege 15 Password 123
R2(Config) # IP domain-name Cisco.Com ↵

R2 . Cisco . Com
R2 . Cisco.Com
Hostname   Domain name
FQDN
fully qualified domain name

الـ Router هيستخدم الـ Key اللي هيشفر بيه

الـ Data من الـ fully qualified domain name

بتاعه اللي هو Rz.cisco.com (اسم الـ Key سيكون FQDN)

نوع Algorithm ← بيعمل التشفير

(Config) # Crypto key generate rsa ?

(512) : —

لو استخدم الـ key كبير الـ Security هتعلى

لكن الـ Performance بتاعة الـ Router هتقل

SSH V1 ⇒ security أقل

SSH V2 ⇒ حجم الـ Key لازم ميقلش عن 768 bit

وسنختار حجم الـ Key هنا 1024.

r2# show crypto key mypubkey rsa

لو عايز اشوف الـ Key اللي اتشفرت بيه الـ Data.

r1# ssh -l Abeer 10.0.0.2

To Connect to R2

R2 * Show IP Int br ↵

R2 * Config t
* line vty 0 15 ↵
* Transport input SSH ↵

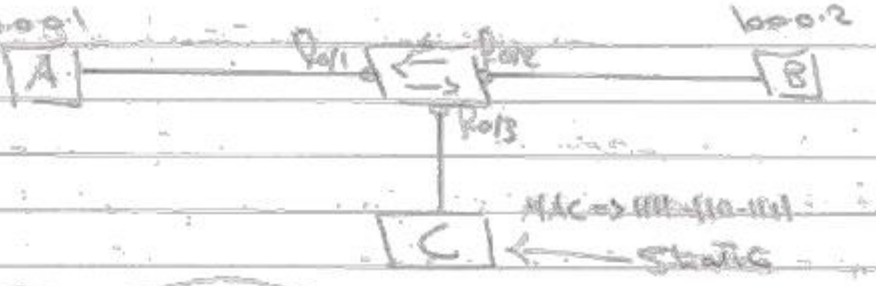
↳ معناه إن كده محدش يقدر يدخل على الـ Router Remotely الا عن طريق الـ SSH

R2(Config) * IP SSH version 2

MAC address table

Switch> ena ↵
* Show mac-address-table ↵
OR * show mac address-table ↵

A ⇒ Ping 10.0.0.2 ↵
نعمل generate لـ traffic بين الأجهزة حتى يتم بناء الـ MAC add table
SW * Show mac-address-table ↵



(Config)# Mac-address-table static ?

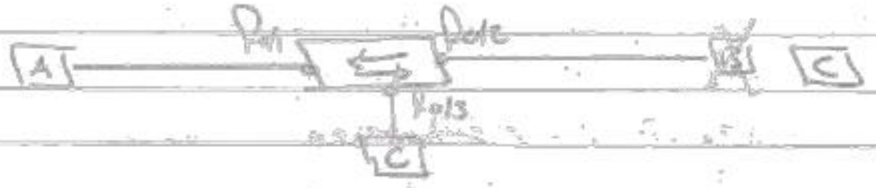
\# Mac-address-table static 1111.1111.1111 vlan1 fa0/3 ↲

لو عاوز احط ال Mac بطريقة Static

\# show mac-address-table ↲

لو ال Source مبعتش اي حاجة في مدة 300sec ال Table يتمسح

(aging time is 300 sec by default)



لو وصلت لجهاز C بدل B كدة ال Mac عنده معلومة غلط.
ومن هنا المشكلة قدامي حل من اتنين.

① استنى فترة ال 300 sec لحد ما ال Table يتمسح

② امسح ال Table بايدي.

\# Clear mac-address-table ?

* ازاي اغير القيمة بتاعة الـ default اللي 300sec ؟؟

sw(config)# Mac-address-table aging-time 900 ↵

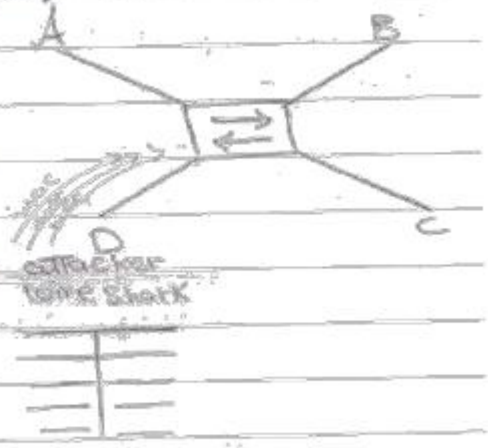
لو لقينا 0 بدل 300 معناها اني باعمل Disable لل Aging Time وهتفضل القيمة موجودة دايماً في الـ Table

sw# show Mac-address-table aging-time ↵

LAN Security attack

① MAC address flooding:-
(MAC add table overflow)

قبل ما يعمل wireshark setup
هيعمل حاجة اسمها Mack add flooding
وهيغرق بعدد Mac كبير جداً
على الـ Table يملى ويشغل الـ Ram بتاعة
الـ sw هيتقل ويبدأ يعامل
الـ sw هيشتغل كأنه hub
وبعدها هيعمل wireshark setup
وهيبقى Man in the middle



* وعلشان احمي نفسي:-

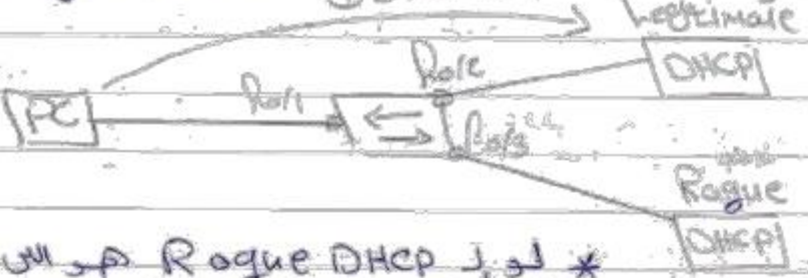
Mitigation:- port security.

اهم نقطة في الـ sec

* ويتم عمل ذلك النوع من الـ attacks عن طريق العديد من الـ tools مثل macof وهي tool موجودة في الـ back tracks.

② Spoofing attack :-

① DHCP Discover
② DHCP offer
③ DHCP Requist
④ DHCP ACK



* لو ال Rogue DHCP هو اللي وزع ال IP مش هيكون الشبكة بتاعته مش في نفس ال Range بتاع الشبكة وقعت.

* لو وزع ال IP في نفس ال Range بس قال للاجهزة ان ال Gateway هو نفس ال IP بتاعه ساعتها اي حد هيحاول يبعت Data هتروحله هو كدة بقى Man in the middle

الحــــل :-

```
sw(Config)#IP dHCP snooping
```

↳ هيوقف اي حد انه ياخد IP من اي DHCP في الشبكة.

```
sw(Config)#int f0/2
sw(Config-if)IP dhcp snooping Trust
```

وبالتالي ال DHCP الموجود على f0/2 فقط هو اللي يستطيع ارسال ال IPs.

↳ شغلها على ال Vlans

* لو عايز اشغلها على Vlan معينة

```
sw(Config)#IP dHCP snooping Vlan 1
```

* لو عندي الـ PC هو الـ Attacker وبيبعت
Mac كتيرة وعايز مقابلها IP لحد مايخلص الـ Pool
بتاعة الـ DHCP 😟
هنحدد الـ Int بتاعه وهنحدد له عدد الـ IP اللي عايزها

sw(Config)# Int f0/1
sw(Config-if)# IP dHCP snooping limit rate 2

③ CDP => Cisco Discovery Protocol
لو فيه 🕴 ولقط الـ CDP هيقدر يعرف معلومات كتيرة
ممكن نعمله Disable على مستوى الـ Router
او على مستوى الـ Int
(Config)# no CDP run
(Config-if)# no CDP enable

④ Telnet attack
بلاها الـ Telnet ونشتغل SSH

Port Security

أنا عندي مشكلة إن جهاز A مثلاً من ممكن يبعت Mac كتير ويوقع الشبكة.
الـ Port Security يعني بحدد الـ Int بتاعه وسامح لو جهاز A بيبعت Data من الـ Mac بتاعه هاقبلها
ولو جاله Data بـ Mac مختلف مش هيقبل.
أو سنستخدم الـ MAC لجهاز الـ A لأنه بطور شرط لإرسال الداتا.

* لو جالك ال Data بـ Mac مختلف

Violation:-

- protect — يعني مش هيقبل ال Data وخلاص

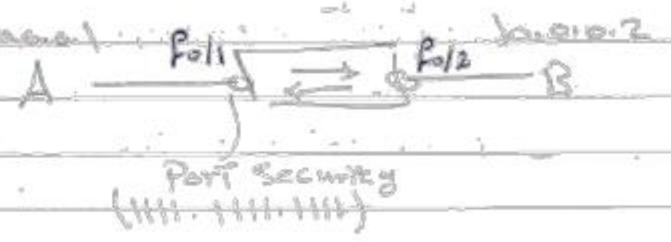
- restrict
  ① مش هيقبل ال Data الغلط
  ② هيزود ال Counter بـ 1
  ③ هيظهر Syslog على ال sw ويقول ال Mac إللي بيعمل Attack

- shut down (default)
  ① مش هيقبل ال Data
  ② هيزود ال Counter بـ 1
  ③ هيظهر Syslog على ال sw
  ④ هيوقع ال Int وهيخليها في حالة اسمها err disabled.
  وعشان الحالة دي تتحل لازم أعمل لل Int shutdown وبعدها No Shutdown

أو نعمل timer لل حالة ال err disabled التي تقع فيها ال int.

« Port security »

lab



Lab => packet Tracer => sw => 2960-24TT

PC 1 => 10.0.0.1

sub => 255.255.255.0

PC2 => 10.0.0.2/24

sw => int f0/1 ↵

sw (Config-if)# switchport port-security ↵

[error]

sw (Config-if)# switchport mode access ↵

Enable بعد ال ← switchport port-security ↵

Port security لل (to enable port security)

sw (Config-if) # switchport port-security mac-add ?

H.H.H

sticky

(1111) => # switch port port-security mac-add 1111.1111.1111 ↵ بعد ما اعمل Enable للـ Port security

mac 1111.1111.1111 مش هيقبل الا Data من

sticky * switchport port-security mac-address
sticky ↵

Mac [illegible] PC [illegible] frame [illegible]
Port Security [illegible]

sw(config-if)* switchport port-security maximum
by default [illegible] mac [illegible] switch [illegible]
bit (1-132) [illegible]

(config-if) * switchport port-security violation protect ↵

PC1 → ping 10.0.0.2
Request time out

sw # show port-security int fa0/1 ↵
int [illegible] port-sec [illegible]

PC1 ⇒ IP config /all ↵
Mac add. [illegible]

* no switchport port-security violation protect ↵
* switchport port-security violation restrict ↵
* do show port-security int fa0/1 ↵

* No switchport port-security violation restricted

* Switchport port-security violation shutdown ←
هلاقي إن الشبكة وقعت

* Show int f0/1 ←
«err-disabled»

① اول خطوة بشيل الـ PC بتاعه واركب الصح
② بعمل shutdown لـ Int وبعدها no shutdown

→ ال led بتاع Switch

- اخضر
  - [illegible] اخضر
  - اخضر ثابت => شغال لكن مفيش Data بتعدي
  - اخضر flash => شغال وفي Data بتعدي
- «amber»
  - يعني الـ Int بايظ او السلك اخرب

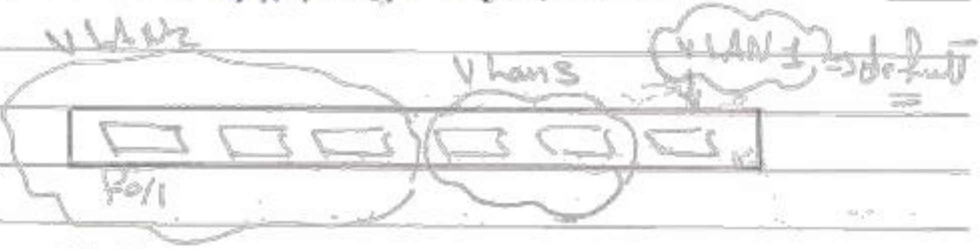
```
sw(Config)# errdisable recovery cause security-violation
sw(Config)# errdisable recovery interval 300 sec
```

or

```
sw(Config-if)# switchport port-security aging time 300 min
sw(Config-if)# switchport port-security aging type (absolute | inactivity)
```

```
sw# show errdisabled recovery
```

"V Lan"
"Virtual LAN"



باخلي مجموعة من الأجهزة عندي في VLAN معينة، وكل مجموعة من الأجهزة تتبع الـVLAN المعينة تستطيع الوصول لبعضها.

لو مسحت على Vlan3 وعملها Delete هلاقي الـ آسة بقت "home less" "number" وكل الأجهزة مش هيبقى عليها Connectivity

ولو عايز أرجع الـ Connectivity قدامي حاجة من اتنين :-

① أرجع الـ Vlan3 تاني وهرجع بالـ آسة اللي كانت عليها

② أحط الـ آسة اللي كانت في VLAN3 في VLAN تانية.

---

① إما أفصل كل دور لوحده (يشبكة لوحده) (غير عملي).

② أو أحط كل قسم في (دور) لوحده مختلف وده Non Security

③ أحط كل قسم في VLAN وده Recommended

بعدما قسمت الشبكة لـ VLAN أل BroadCast
هيوصل فقط للأجهزة في الـ VLAN تباعته.

* Security
* Segmentation,

يعني قسمت الشبكة بناس كل Vlan ثانية تتصل فقط على
ضمان الـ security

* managability

علشان Vlan تستطيع الوصول V lan لازم يتم Routing
بعض هيشوفوا بعض كـ UniCast مش BroadCast

(BroadCast is not evil) انا بأقلل فقط الـ
BroadCast domain

* Managability: هقدر manage الشبكة بتاعتي
بأسلوب اسهل.

* الهدف الرئيسي من تقسيم الشبكة لـ VLANs هو تقسيم الشبكة
لأكثر من broadCast domain

« VLAN Charactristics »

***VLAN ID:-**

ال VLAN باعملها Create ب رقم والرقم ده ممكن يكون واحدة من ال تنين

Normal	Extended
- VLAN 1 "default"	- VLAN 1006 → 4094
- VLAN 2 → 1001	
- VLAN 1002 → 1005	

* ال VLAN 2→1001 دول اللي انا اقدر ك admin اطبقها عندي على ال switch

* ال VLAN 1002→1005 اتقرضوا خلاص وكان بيستخدم في ال FDDI وال Token Ring

Extended ⇐ بيستخدم شركات ال ISP على ال transparent sw

وكل VLAN ليها رقم واسم واي VLAN باعملها create عن طريق الرقم

مثلا VLAN 2 ⇒ HR

اذا لم احدد لها اسم {
VLAN3 ⇒ VLAN 0003
VLAN 20 ⇒ VLAN 0020
}

"Types of VLANs"

لو غيرت A لـ Port2
المفروض انه تنقل [illegible] VLAN

MAC	VLAN
A	10
B	20

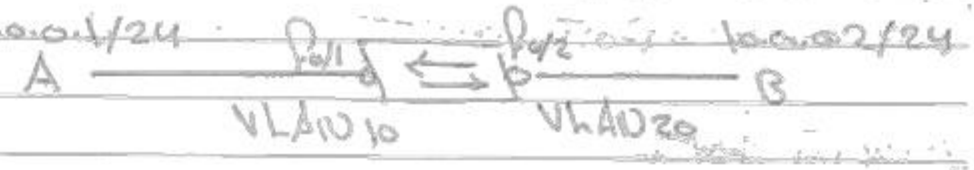
بـ create الـ Table الـ MAC
الـ Database بين الـ PC والـ VLAN
[illegible]
[illegible] VLAN [illegible]

"Voice VLAN"

IP Telephony

[illegible] الـ Telephone والـ PC في نفس الـ VLAN
[illegible] Setup [illegible] PC [illegible] Tele
[illegible] level [illegible]

"VLAN Config"



Packet Tracer:

switch> en ↵

switch# Show VLAN ↵ (معلومات تفصيلية لـ VLAN)

\# Show VLAN brief ↵ (معلومات مختصرة)

علشان اعمل VLAN Configuration فيه طريقتين

Vlan database

~~[illegible]~~

~~Not Recommended~~

switch# Vlan database

sw(Vlan)# Vlan 2

sw (Vlan)# Vlan 3 name HR

~~Vlan 3 added~~

~~Name: HR~~

لازم اعمله Exit علشان تضاف في ال Vlan database او اعمله Apply

وبالتالي هيتفعل ال Vlan وهيبقى في نفس الوقت

"الي استخدمت في Control Z مش هتضاف"

Config mode

\# Config t

\# Vlan 10

\# exit

\# Vlan 20

\# Name SALES

لو عايز create الـ VLAN في سطر واحد ⇓

\# Vlan 10,20,30-40

من 30 لحد 40 ← واحدة واحدة

(Config)# int fo/1 ↵
(Config-if)# switchport mode access ↵ بعطله تبقى كده
(Config-if)# switchport access vlan 10 ↵ Vlan 1

(Config)# int fo/2 ↵
(Config-if)# switchport mode access ↵
(Config-if)# switchport access vlan 20 ↵

لو عايز أوزع 100 ports على vlan معينة

For exg- ① fo/3 : fo/6 => vlan 2
② fo/8, fo/10, g1/1 => vlan 4

⇓

① Switch (Config)# int range fo/3 - 6 ↵
switch(Config-int-range)# switchport access mode
sw (Config-int-range) # switch port access vlan 2 ↵

② Switch (Config)# int range fo/8 , fo/10 , g1/1 ↵
sw (Config-int-range)# switchport mode access ↵
sw(Config-int-range)# switchport access vlan 4 ↵

Switch (Config)# no VLAN 4 ↵
بعمل Delete لـ Vlan4 الـ int
هيبقوا Homeless

لـ Vlan يعمل ما يحدث Create يتم حـ
تب لـ Flash:Vlan.dat

شيل لـ قتـ الي قب لـ Vlan موجودة تحت
NVRAM: Startup-Config.
Switch
* علشان ارجع لـ على لـ default
اعمل Reset لـ Switch
لازم ٣ خطوات.

Enable mode*
① erase startup-config ↵
② Delete Flash:Vlan.dat ↵
③ Reload ↵

(Trunking)

vlan 1

بس ازاي الـ SW يعرف إن الـ Data في VLAN معينة
بيتم عن طريق Trunking Protocol

* Trunking Protocols وظيفتها إنه بيمسك الـ frame
من عند الـ SW اللي هيبعت ويحط عليه Sticker الـ Vlan
اللي هيعرف توصله.

* بيوجد نوعين من الـ Trunking protocol

ISL	dot1q = 802.1Q
- Cisco properiary	- IEEE standard
- encapsulate frame	- tags frame
- Doesn't support Native VLAN	- support Native VLAN
	« تقريباً ... »

(ISL) inter switch link

حجم الـ packet ⇐ By default ⇐ 1500 byte

MTU ⇒ Maximum Transfer unit

الـ cisco بيقدر يتعامل مع الـ frame أقصاها 1518 byte Giant

وأدناها 64 byte Runt

لو وصلتني frame أكبر من 1518 يعملها drop

ولو أقل من 64 يعملها Drop

* الراوتر بيقوم بعمل fragmentation لـ packet إذا تعدى حجم الـ MTU يمكن أن تكون لوجيا الـ ethernet لا يستطيع

(802.1Q)

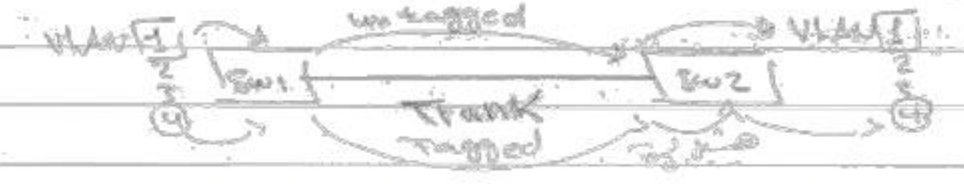
بيزود حاجة بسيطة وهي Tag في نص ويبقى فيها الـ VLAN ID

ويزود FCS علشان يعمل error detect على الـ Data الجديدة

مثل الـ Tag كان.

Native VLAN:-

By default Native VLAN = Vlan 1



الـ Native Vlan لازم يبقى واحدة على الـ Switches

Cisco ⇐ Recommend أن الـ Voice يبقى في الـ Native Vlan

علشان الـ Voice أصلا تقيل.

* من خطورة الـ native VLAN أنه ممكن يحدث attack على السويتش اسمه double tagging لذلك لا يفضل استخدام الـ native VLAN أصلا أو عمل tagging لها.

access int: belongs to only one Vlan
Trunk int: belongs to all Vlans.

DTP
"Dynamic Trunking Protocol"

Int => 1 access
2 Trunk

default <= Dynamic -> auto
-> desirable

3550 -> dynamic desirable   3560, 2960 -> dynamic auto

بيبعتوا لبعض كل 30sec بيسألوا بعض هيشتغلوا ازاي
عندك استعداد تشتغل Trunking ولا لأ

auto =>   كل مره مستني التاني يبدأ negotiation

desirable =>   انا هبدأ البداية.

لو عملت الـ اتنين Trunk Int Recommended يبقى اوقف
الـ DTP

Lab8-

* Show int Trunk ↵ — لو عايز اعرف ال Int شغالين Trunk ولا لأ

* Show int fo/1 trunk ↵ — لو عايز اعرف ال Int ده شغال trunk ولا access ولا Dynamic auto ولا Dynamic desirable

* Show int switchport ↵ — كل المعلومات عن
او * Show int fo/1 switchport ↵ — ال Int شغال ايه :
administrative mode: dynamic auto
operational mode: access

Sw1 * Int fo/1 ↵
(Config-if)* switchport mode ?

H.W

* Show Int Trunk ↵

Hard Code — علشان اوقف ال DTP Protocol الي بيشغل ال Int = Trunk ولو عايزه اوقفه بالأمر
(Config-if)* Switchport nonegotiate ↵
Sw # show dtp ← to know general info about DTP

VLAN Hopping

- Double tagging — using native VLAN
- Switch spoofing — using DTP

ازاي اغير الـ Native VLAN ؟؟

sw1 * int f0/1 ↵
sw1(config-if)* switchport trunk ?
allowed
native
* switchport trunk native vlan 2 ↵

sw2 ⇒ نفس الكلام
لازم اغير الـ Native Vlan في الاتنين.

* show int trunk ↵

الـ Trunk بيشيل كل الـ Vlan لكن بايدي
امنع اصحاب الـ Vlan اللي بحددها

(config)* int f0/1
(config-if)* switchport trunk allowed vlan2 ↵

(config-if)* switchport trunk allowed ?
(word) add all none remove except

- all VLANs are allowed through the trunk int by default
- but we can specify specific VLANs

" Inter VLAN Routing "

بأعمل Routing بين ال VLAN علي شان كل VLAN
تشوف التانية بس كـ unicast مش BroadCast.

* inter VLAN routing is done using a L3 device , router or a L3 switch.

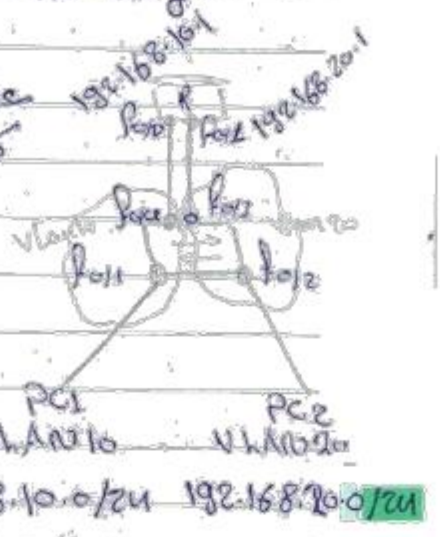
① Router

* Traditional inter-VLAN Routing

علي شان اعمل ال Routing لل VLAN لازم
كل VLAN تكون في Network ID مختلف

مش بتستخدم ال VLAN كتيرة

اذا كان يوجد عدد كبير من ال VLAN سنحتاج
int على الراوتر لكل VLAN.

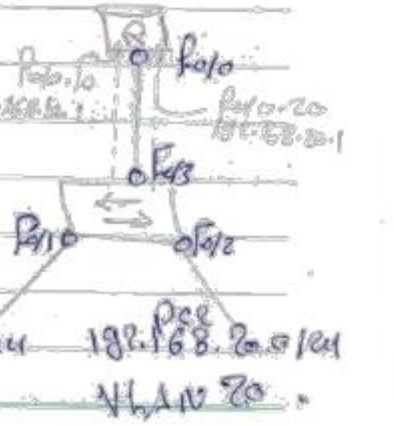


* Router-on-a-stick

هاجي على ال Router وأعمل IP لل Int f0/0
وأعمله No shut وأجي على ال Router وأعمل
subinterfaces ⇐ وأدي لكل واحدة IP

f0/0.10 => 192.168.10.1
f0/0.20 => 192.168.20.1

مضيفة بين ال Int بين ال R وال sw
هيبقى Trunk



علشان الـ Router-on-stick يشتغل مع الدوام؟ بأخذنا
محكومين ب FEth او GEth وكمان عيوبه انه يعمل يسبب Congestion
في الشبكات الكبيرة

Labs- sw# int Fo/1 ↵
sw (Config-if)# Switch mode access ↵
sw (Config-if)# switchport access vlan 10 ↵

sw (Config)# int Fo/2
sw (Config-if)# switchport mode access ↵
sw (Config-if)# switchport access vlan 20 ↵

sw (Config)# int Fo/3
sw (Config-if)# switch port mode Trunk ↵

Router# int Fo/o
(Config-if)# no shutdown
Router(Config)# int Fo/o.10 ↵ → VLAN
R (Config-subif)# encapsulation dot1 (10)
R (Config-subif)# ip add 192.168.10.1 ▿ 255.255.255.0 ↵

R (Config)# int Fo/o.20 ↵ → VLAN
R (Config-subif)# encapsulation dot1 (20)
R (Config-subif)# Ip add 192.168.20.1 ▿ 255.255.255.0 ↵

PC ⇒ IP ⇒ subnets ⇒ Gatway

pc1 ⇒ 192.168.10.100/24
gateway → 192.168.10.1

PC2 ⇒ 192.168.20.100/24
gate-way → 192.168.20.1

From PC1
Test => Tracert 192.168.20.100
or Ping 192.168.20.100

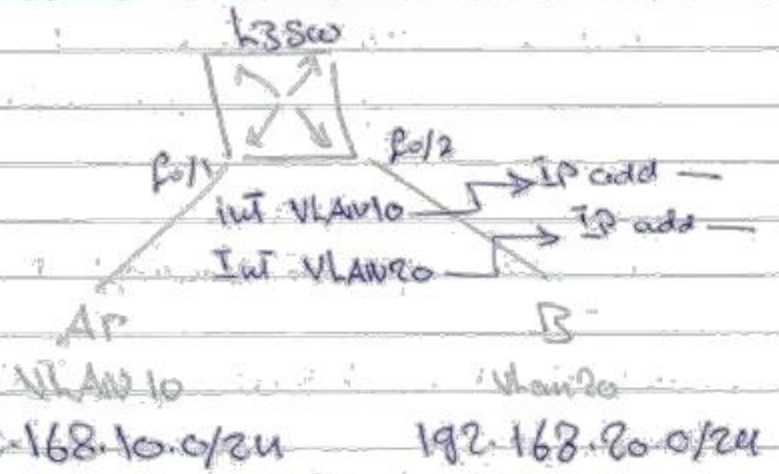
② افضل Senario لل Routing هو ال L3 sw

* لما بحط IP على ال sw بحطه على Int اسمه
SVI اسمه!

Switched Virtual
Interface

sw(Config)## int Vlan 1
sw(Config-if)## IP add 10.0.0.1 255.255.255.0
sw(Config-if)## No shut

معنى كدة VLAN هي ال mangement يعني اسمها
VLAN
بتاعة VLAN1 هي اللي هتعمل Telnet على ال sw



بعد الـ Configuration لـ الـ ip

** sw(Config)# ip routing ↵

⇒ عشان أعمل Enable لـ Routing

lab

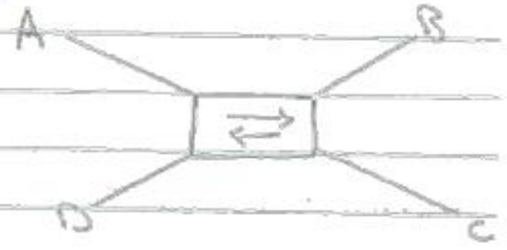
```
sw(Config)# int Vlan 10
sw(Config-if)# ip add 192.168.10.1 255.255.255.0
sw(Config)# int Vlan 20
sw(Config-if)# ip add 192.168.20.1 255.255.255.0
sw(Config)# Vlan 10,20
sw(Config)# ip routing
sw(Config)# int f0/1
sw(Config-if)# switchport mode access
sw(Config-if)# switchport access Vlan 10
sw(Config)# int f0/2
sw(Config-if)# switchport mode access
sw(Config-if)# switchport access Vlan 20
```

* Routing is enabled on router but disabled on L3 sw by default

« Switching »
Revision

Switch Jops:-

① MAC Address learning:-



اول Frame بيجيلو Flood عادي
لـ Int اللي جه منه Data
ويدونه بـ Switch لـ Mac add table

② Forward decision:-

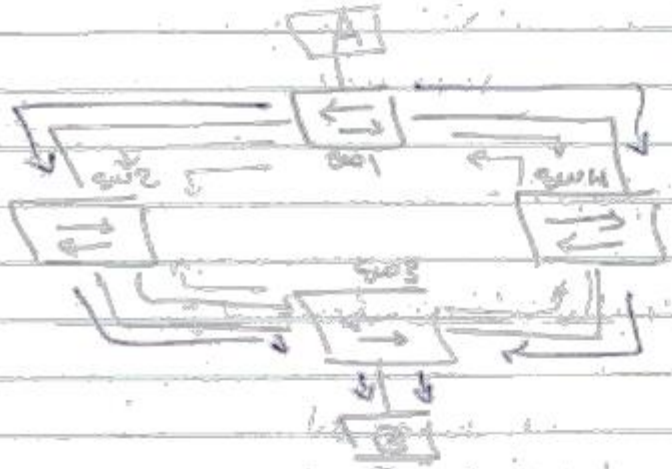
int	MAC
fo/1	A
fo/1	B

ا لو لقي ال sw ال Source
و ال Destination ← Connected
على نفس الـ Int ــــ ينفذ
هيعمل Block لل Int
للمرار frame تتجبت ويفتح
لـ Int تاني

③ prevent switching loops Caused by redundancy.

لو حصل switching loop فلازم حل الا إني اعمل Reset

الحل مع الي على اسـ بالمرة



* في حالة ال (Redundant Topology) هيبقى عندي عرضة إني يبقى عندي

switching loop . لو ال PC A بعت Broadcast

هيحصل عندي Broadcast Storm

مشاكل ال Redundant Topology :

① Broud Cast Storm :-

② multiple frame copies :-

في حالة ال unicast هيوصل ال frame مرتين لل Destination

③ Mac address table instability :-

مايعرفش يحدد:
هيوصل لي من ال 2 int. Sw
ساعتها ال Mac Add Table ⇐ instable

SW3

Int	Mac
~~Fa0/1~~	~~A~~
Fa0/2	A

أول حاجة الـ sw عليه protocol إسمها STP
وده اللي هيوقف الـ switching loop

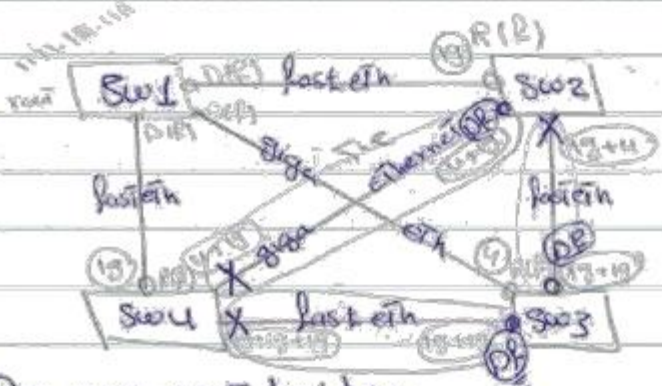
* هيخلي الـ frame تمشي في طريق واحد بس يعني ولو الطريق
ده وقع ← التاني الـ sw اول STP هيشغل الطريق التاني

STP

Spanning tree protocol

(* at startup)

① one root bridge per network
(bridge → switch)



② one rootport per non-root bridge.
③ one designated port per segment
④ block all other.

① عندي sw واحد بس هو اللي هيبقى root switch
كل sw عندي عليه حاجة إسمها BPDU
BPDU "bridge protocol data unit"

2 byte	6 byte
Priority	Mac add.

By default = 32768

اول ما ال sw هتقوم مع بعضها هـ كل sw هيقول انا
ال ROOT ساعتها هيحصل tie اللي هيحصل ال Tie
ال Priority عن طريق اقل قيمة بس المشكلة إنه ال sw
كلها قيمة By default = 32768 ساعتها اللي هيحلها هو
ال Mac add وال ROOT هيبقى ال sw صاحب اقل Macadd.

---

* لو الشبكة كلها شغالة و بقت Stable ودخل sw جديد في الشبكة وعليه Mac اقل ساعتها ال sw الجديد هو اللي هيبقى ال root.
* ال sw root اول ما يعرف انه root كل ال Int اللي عليه ساعتها هتبقى في حالة اسمها Designated forward "DFn"
وكل ال Data هتعدي من عليه.

© كل ال sw التانية هتبقى (non-root switch) وساعتها كلها هيبقى عليه Int واحد اسمه root port.

Link speed	Cost "IEEE"
10 Gb/s	2
1 Gb/s	4
100 Mb/s	19
10 Mb/s	100

هيبدأ يحسب أقل سوج قيمة لـ cost على شان يوصل لـ الـ root
الـ Int اللي هيجي عن طريقه أقل cost هيعتبره الـ
Int ده هيبقى هو الـ root Int وهيبقى في حالة
الـ Root forward (RF) وبيعدي ويسمح لـ Data تعدي
من عليه

---

③ كل سلك هيبقى عليه D.Port
هيبص على السلوك اللي مش عليها D.Port وهيقارن عن طريق
الـ Cost بتاع الـ sw على شان يوصل بالـ root وهيختار
الأقل.
لو حصل Tie هيفصل عن طريق الـ Int اللي مربوط بـ sw
ليه Mac أقل.

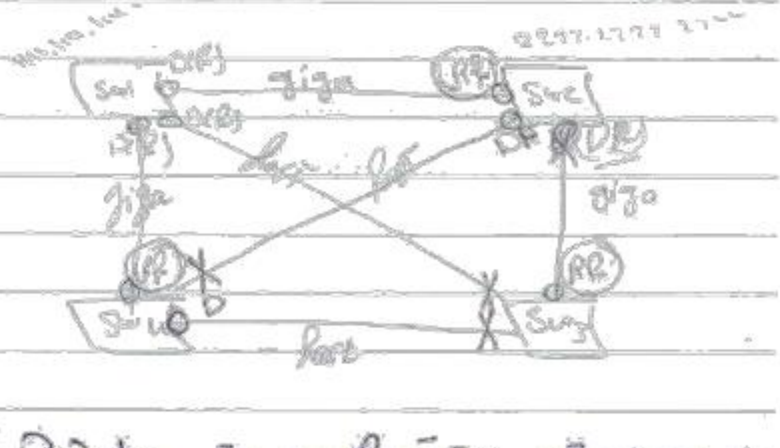
---

④ الـ Int اللي متطبقش عليها Rules هيعمله Block

Logically down.

وهيبقى وضعه إسمه Logically down.

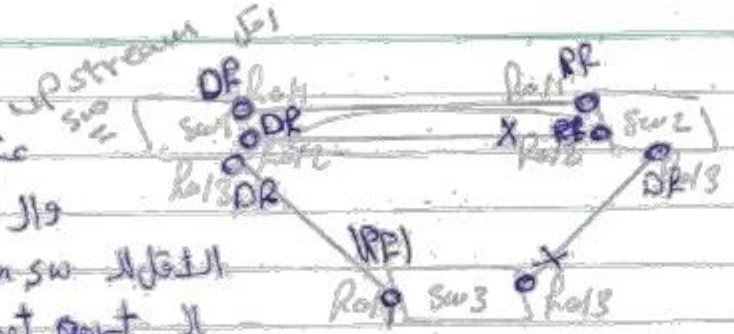
Ex:-



* بعدما يبقى سوج Root هيبعت BPdu كل 2 sec عن طريق
الـ D(P) الـ sw ويستقبل باقي السويتشات الـ Root
port عن طريقها مرسلها الـ designated port.

Ex

عند حدوث tie في الـ 1st
والـ MAC add فإن الـ port ID
الأقل الـ sw upstream هو الذي سيكون
الـ root port.



x ما Convergence — الـ root switch بيبعت hello كل 2 sec.

- STP port states:-

① Disabled => بيعني انه اتعمله shutdown بإيده
② Blocked
③ listening => بيـ listen للـ BPdu لمدة 15sec
وبعد كده هيدخل لحالة الـ learning
④ Learning => بيبدأ يتعلم الـ Mac add ويحطها في Table
لمدة 15sec وبعد كده يتحول لـ forward
⑤ Forward =>

« BPDU Timers »

* Hello time: بيتبعت كل 2sec By default

* Forward delay: الفترة اللي بيقعد فيها الـ port وهو بيتحول من Blocked لـ forward ⇐ 15sec+15sec=30sec

* Maximum age:-
= 10 * hello = 2 * 10 = 20 sec.

*** at change**

① If root bridge goes down:-

all other switches go to blocking state for 20 sec then → go for listening state for 15 sec then → to learning Mac for 15 sec ⇒ 15+15+20 = 50 sec

② If any other change happened

all routers goes directly for listing for 15 sec then ⇒ goes to learning for 15 sec ⇒ 15+15 = 30 sec.

lab:

* STP is enabled by default on all Cisco SWs.

* Show spanning-tree ↵

كل ما تعمل sw هيجي لـ root

SW1 # Config t ↵

SW1(Config) # spanning-tree ?

SW1(Config) # spanning-tree vlan 1 ?

SW1(Config) # spanning-tree vlan 1 (لو الـ STP Enabled على VLAN 1)

SW1(Config) # spanning-tree vlan 1 root ?

SW1(Config) # " " " " primary

SW1 # Show spanning-tree ↵

هتلاقي إن تغير الـ Preiority

priority is increments of 4096

* spanning-tree vlan 1 priority 4096

PVST => Per-VLAN STP (Default on Cisco SWs)
supports ISL only

PVST+ => supports ISL and dot1q — كل STP بتعمل على vlan لوحدها

---

extended System ID :-

default — VLAN ID

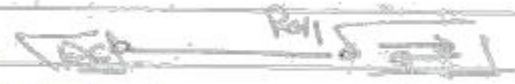
VLAN1 => Priority => = 23768 + 1 = 23769

Vlan 10 => " => = 23768 + 10 = 23778

* عند تغيير الـ priority عن طريق أمر root primary فإنه shortcut للأمر الـ priority.

STP enhancement : تحسينات

* Port fast : خاصة PC Connecting to بتحصل
من Block إلى Forward في No time "التحول".
، إذا حدث تغيير على السويتش
فإنه يرسل TCN لكل السويتشات



مرتبطة بـ Int لعمل flush لل MAC table . ولكن حدث تغيير على
int مرتبط بـ pc لا يوجد داعي لعمل flush على مستوى الشبكة كذلك لا يوجد
مخاطر من جعل ال int يتحول من BLK إلى FWD
مباشرة دون التأثير من حدوث switching loop.

* int fa0/1
* Do show spanning-tree
* Shut down
* no shutdown
* spanning-tree portfast
* switchport mode access.

وإذا استلم السويتش BPDU على ذلك ال int سيعمل disable لل port fast.

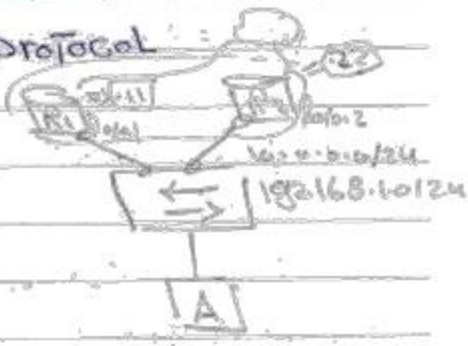
* RSTP => rapid - STP

- STP => Blocking => listing (15 sec) => Learning (15 sec) => forward
  Max age = 10 * hello = 20 sec.
- RSTP => Discarding => learning (15 sec) => forward
  max age = 3 * hello = 6 sec
  خلي بس تعدل hello

802.1D => STP
IEEE

802.1w => RSTP
IEEE

Redundancy protocol



لو الـ R1 (down) عاوزين الأجهزة تبعت
على R2 لوحدها وممكن طريقة
ما عرف الـ Protocols

1- HSRP ⇒ Hot standby router protocol
((Cisco Propritary))

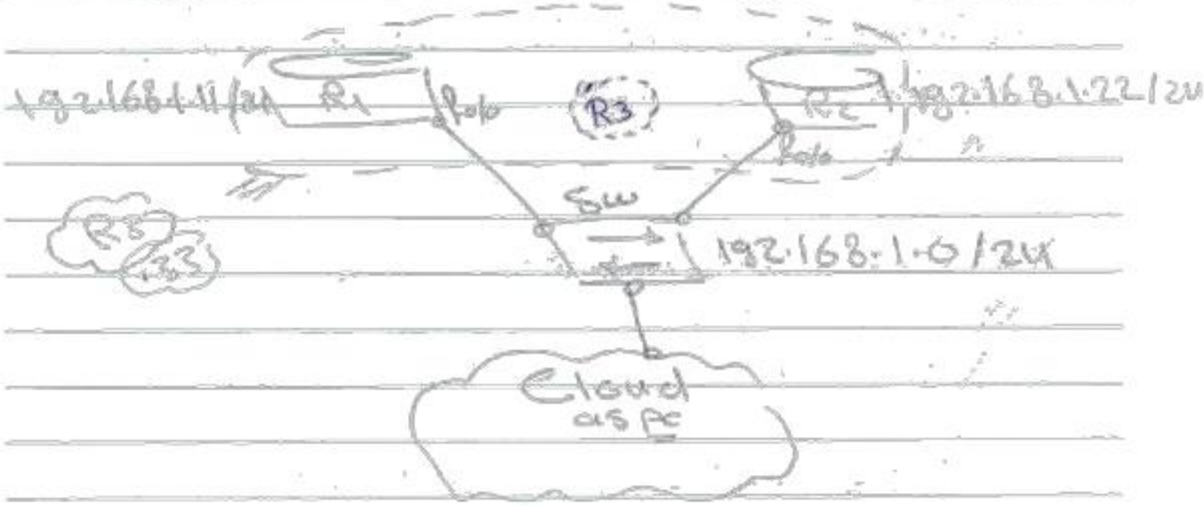
2- VRRP ⇒ Virtual router redundancy protocol
((IEEE Standard))

3- GLBP ⇒ Gateway load balance protocol
((Cisco Propritary))

هاجي على R1, R2 وهاحطهم في Group وهطلع
منهم Router وهمي وهيبقى ليه IP و MAC بيه
و الأجهزة هتشاور عليه عن طريق ال Gateway،
وضامن لو R3 هيشاور على R1 يبقى الأجهزة متوصلة
على ال Internet عن طريق R1 ولو R1 وقع مش R3
هيشاور على R2.

Lab: Lsow نفس التصميم على الـ R هو المتبع لدى

GNS ⇒ Run as administrator



r1 (Config)# int f0/0 ↵

* Ip add 192.168.1.11 255.255.255.0 ↵

No shut ↵

r2 (Config)# int f0/0 ↵

* IP add 192.168.1.22 255.255.255.0 ↵

No shut ↵

r1 (Config)# f0/0 ↵

* Stand by ▽ 1 ▽ ?   ip address Group ip ? لعمل

* Stand by ▽ 1 ▽ IP 192.168.1.33 ↵   ↵

└ The IP of the virtual router.

r2(config) int f0/0
* standby 1 IP 192.168.1.33 ↵

r1(config)# line vty 0 4 ↵
* pass 123 ↵
* login ↵

r2(config)# line vty 0 4 ↵
* pass 123 ↵
* login ↵

PC => cmd => Telnet 192.168.1.33

هلاقي انه بشاور على R1 على اساس هو ال Active.

ping 192.168.1.33 -t ↵

* R1(config-if) #shut down ↵

هلاقي Ping واحدة هيبان وقفت و هيرجع نفسه
تلقائي على R2 و R2 هو اللي بقى Active

⇐ أي R هيبقى Active والتاني Standby ؟؟

الـ R اللي هيقوم الأول هو اللي هيبقى Active.
ولو قاموا في نفس الوقت اللي هيحل الـ Tie هيبقى الـ
Priority ⇐ اللي ليه أعلى Priority هو الـ Active
بس هيحل الـ Priority ⇐ (100) ⇐ By default
يبقى اللي هيحل الـ Tie الـ R اللي الـ IP بتاعه
أعلى هيكون هو الـ active والآخر standby.

r1 # Show Standby ↵

r2 # Show Standby ↵

Mac ⇒ 0000.0c07.ac01

AUI ⇐ ده هيفضل ثابت ده

HSRP ⇐ ده هيفضل ثابت للـ

⇐ رقم الـ Group بالـ Hexa

يعني لو رقم الـ Group 10 هيكتبه 0A

Hello time ⇒ 3 sec

hold time ⇒ 10 sec

يعني كل 3sec الـ R بيبعتوا لبعض Hello علشان يعرفوا بعض إنهم شغالين

Preemption disabled (الاستيلاء)

r2(Config-if)# standby 1 ?

* standby « 1 » preempt

يعني R2 لما يقوم يرجع هو الـ Active ، يشتغل على طول

فيقعد بالـ Priority ، الـ R اللي الـ Priority بتاعه أعلى

* standby « 1 » priority 150 ↵

بعد عمل enable لـ preempt على الراوتر اللي له الـ Priority الأعلى

سيكون هو الـ active مبدئياً بعد ما يرجع up مجدداً .

لو عندي link بين الـ R والـ ISP ووقع فاتصالي راح

الـ Int اللي داخل على ISP اول ما يقع يقلل الـ Priority

بـ 60 عشان R1 يصبح الـ Active

بنفرض ان الـ int loop 2 هو اللي بيربطني بالـ ISP .

r2(Config)# Int loop2 ↵

r2(Config-if)# IP add 2.2.2.2 255.255.255.255 ↵

---

r2(Config)# Int f0/0 ↵

r2(Config-if)# standby 1 track loop2 (60) ↵

← يقلل الـ Priority بـ 60

* preempt should be enabled in conjunction with tracking ints.

r1(Config-if)# standby 1 preempt ↵

مشكلة الـ HSRP إن الـ timers عالية

hello ← ← hold time

r2(Config-if)# standby 1 timers (1) (3)

ويمكن وضعها بالـ msec ولكنه غير مستحب .

- VRRP ⇒ هو هو ال HSRP مع بعض الفروق

1. "IEEE Standard"
2. hello ⇒ 1 sec
3. hold ⇒ 3 sec + skew time.
4. preempt ⇒ enabled by default.
5. R_3 ⇒ ينفع يأخذ IP زي ال IP بتاع R من نفس ال Group بعكس ال HSRP

⇒ lab

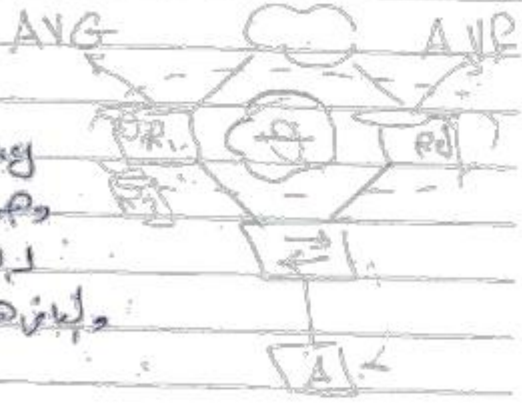
R1(config-if)# vrrp ?

vrrp 1 ?

do show vrrp ↵

- GLBP ⇒ Cisco propriatary
"Gateway load balance"
زي ال HSRP بس الفكرة إن انا اعمل load balance

AVG ⇒ بيختار R من اللي
ويعمله AVG
Active virtual Gateway
وهو مسؤول عن توزيع ال MAC
ل ال PC
والباقي AVF ← Active virtual forwarder.



fo/o ↵
GLBP 1 ?

R(Config-if)#glbp 1 ?

AVG | بيتحدد بأعلى Priority |

* weighting -> " load balance " ال بأوزع عن طريقه

" Channel Group "
etherchannel
portchannel

الفكرة إني أخلي ال 8 interfaces بيشتغلوا
" equal cost " بين هاتين يبعت ال frame على
load Balance الفكرة ال frame على ال 8 interfaces
ولازم على إدائة.

ممكن إني أوصل ب 2 sw من 8 لحد ...

labs:-

Sw2(Config)
* Int range f0/0 0-03
* shutdown
* channel- Protocol ?

1 channel protocol نوعه

- on → (hard code eth channel) Int مع بعض بدون

- LACP "link aggregation control protocol"
- PAgP (Port aggregation protocol) — Auto negotiation
  ↑ cisco proprietary

labs

sw1(config-if-range)# channel-group 1 mode ?

LACP → active = desirable
  → passive = auto

PAgP → auto = passive
  → desirable = active

\# channel group 1 mode on
\# no shut
⇒ sw2 → نفس الكلام
  no shutdown

sw1# show spanning tree
\# show etherchannel 1 => علشان اشوف الحالة
  summary
  (SU) ← يعني شغالة

ال STP بيتعامل مع ال channelgroup كأنه int واحد هو ال port channel.

((wireless))

wireless Tech. اتصال بين ٢ شبكات لازم اوصلها شبكة (شركة حول ، بلارة)

	Ethernet	wireless
IEEE	802.3	802.11
media	Copper-Glass	air
data format	electricity-Light	Radio waves

((wireless Topology))

- Ad-hoc (IBSS)
  Independent basic service set.

  - No Access point
- infrastructure
  - BSS
    Basic service set
    - one Access point
  - ESS
    Extended service set
    - more than one Access point.

لازم الـ user في منطقة الـ overlap تكون قوة الشبكة
من 10 → 15%

ناخد الـ Config على الشبكة نفسها Service Set =S
ويبعتها الـ Broadcast على الـ frame اسمها Beacon
frame

Recommended مش مفيد تتعامل على شان الـ Security
واعمل Disable لل Beacon frame

802.11 (2.4 GHZ (frequency) - 1,2 Mbps (speed))

802.11a (5GHZ (frequency) - 54 Mbps (speed))

802.11 b (2.4GHZ - 1,2,5,11 Mbps)
↳ spread spectrum

802.11G (2.4GHZ - 54Mbps)

b,G => Compatable مع بعض

CSMA / CA ⇒

↳ Collision avoidance

Freq. بيتجنب الـ Callision عن طريق بيبعت على
و بيشغل على Freq

Bluetooth ⇒ V1 ⇒ 2.4GHZ → 10m
1Mbps

↳ V2 ⇒ 2.4GHZ → 35m → 2Mbps

---

wireless signal attenuation:-

- interference
- environmental variables العوامل الجوية - أمثلة
- Antenna type and length
طولها ونوعها

Wireless Sequrity:

- war drive ⇒

إزاي احمي نفسي من انواع الـ Attack

عن طريق الـ MAC add ⇐ يعني اسمح لـ الـ Mac اللي هيطلع نت

٤ عن طريق الـ Authentication بالـ Key اللي
على شبكة الـ wireless بيكون
وعندي نوعين من التشفير ← wep
"ضعيف جداً" وضعيف جداً
(56 bit) وبيعتمد على
نوع encryption ضعيف جداً
"TKIP"

WPA, V1, V2
أعلى sec
وبيضرب برضوا
والـ dynamic Key
بيتغير على طول.

٥ security applianse
أجهزة بتعمل لـ data أو IDS, IPS